UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/741,691	12/15/2000	Vipin Samar	OR00-14201	6542

51067 7590 09/22/2006

ORACLE INTERNATIONAL CORPORATION
c/o PARK, VAUGHAN & FLEMING LLP
2820 FIFTH STREET
DAVIS, CA 95618-7759

EXAMINER
SON, LINH L D

ART UNIT	PAPER NUMBER
2135	

DATE MAILED: 09/22/2006

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/741,691	SAMAR, VIPIN	
	Examiner	Art Unit	
	Linh LD Son	2135	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *26 June 2006*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1,4,7-12,15,18-23,26 and 29-33* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1,4,7-12,15,18-23,26 and 29-33* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☐ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

1. This Office Action is responding to the Amendment received on 06/26/2006.

2. Claims 2-3, 5-6, 13-14, 16-17, 24-25, and 27-28 are canceled.

3. Claims 1, 4, 7-12, 15, 18-23, 26, and 29-33 are pending.

Claim Objections

4. Claims 1, 12, and 23 are objected to because of the following informalities: The amended limitation "*looking up **a private key(#1)** for the user at the signature server based on the user identifier and the application identifier, wherein looking up **a private(#2)** for the user based on the user identifier and application identifier prevents a user who is allowed to access a second application, but who is not allowed to access the application being used...*" recites "a private key" again which allows access to a second application, but not the application being used or first. By the claim language, Examiner interprets "**a private key(#1)**" as a first private key and the "**a private(#2)**" as a second private key. Appropriate correction is required.

Claim Rejections - 35 USC § 103

6. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

7. Claims 1, 4, 7-12, 15, 18-23, 26, and 29-33 are rejected under 35 U.S.C. 103(a) as being unpatentable over Dickinson et al, US Patent No. 6853988B1, hereinafter "Dickinson".

8. As per claims 1, 12, and 23:

Dickinson discloses "A method for facilitating the delegation of operations involved in providing digital signatures to a signature server, the method comprising:

allowing a user to authenticate the signature server" in (Col 7 lines 7-30);

"receiving the message from the user at the signature server, the message including an item to be signed on behalf of the user by the signature server, a user identifier which identifies the user (userID) (Col 7 lines 7-30), and an application identifier (certificate type: RSA, ELGAMAL, or the like in Col 21 lines 25-40) which identifies the application being used" in (Col 47 lines 30-45, Col 21 lines 1-50, and Col 21 line 60 to Col 22 line 17);

"authenticating the user at the signature server" in (Col 7 lines 7-30, and Col 47 lines 40-45):

"determining whether the user is authorized to sign the item by communicating with an authority sever that is separate from the signature server" in (Col 21 lines 1-50, and Col 21 line 60 to Col 22 line 17);

"looking up a private key for the user at the signature server based on the user identifier and the application identifier;" in (Col 7 lines 7-15, and Col 21 lines 42-50), wherein looking up a private key for the user based on the user identifier and anpplication identifier prevents a user who is allowed to access a second application, but who is not allowed to access the application being used, from gaining access to the application being used" in (Col 21 lines 25-40, Col 21 line 36, Col 21 lines 42-60, and Col 20 lines 55-67) [Both the user identification (Col 7 lines 7-30) and the application identification (certificate type in (Col 21 lines 25-40)) get authenticated to retrieve the private key corresponding the certificate owned by the user (Col 21 lines 43-60). Each certificate corresponds to a private key and each certificate correspond to a cryptographic application or communication protocol, or protocol. Thus, one private key corresponds to a first certificate cannot be used for a second certificate. (Col 20 lines 55-67)]; and

"signing the item with the private key for the user" in (Col 47 lines 40-47).

However, Dickinson only teach of sending the message and the authentication data to the vendor and the trust engine" in (Col 47 lines 30-45). Dickinson does not specifically pointed out which one is sent first.

Therefore, it would have been obvious for one having ordinary skill in the art to modify Dickinson's teaching to authenticate with the server first before sending the message for signing to the signing server for the purpose of reducing the requesting for service memory in the server and further decreasing the possibility of compromising the message and the signature by the party that is mistakenly sent to.

9. As per claims 4, 15, and 26:

Dickinson discloses "The method of claims 1, 12, and 23, wherein determining whether the user is authorized to sign the item involves looking up an authorization for the user based upon an identifier for the user as well as an identifier for an application to which the user will send the signed item" in (Col 21 lines 43-67).

10. As per claims 7, 18, and 29:

Dickinson discloses "The method of claims 1, 12, and 23, further comprising returning the signed item to the user so that the user can send the signed item to a recipient" in (Col 48 lines 23-30).

11. As per claims 8, 19, and 30:

Dickinson discloses "The method of claims 1, 12, and 23, wherein the method further comprises configuring the signature server to accommodate a new user by: receiving a request from an authorized entity to add the new user" in (Col 18 lines 36-55); "generating a key pair for the new user, including a new user private key and a new user public key; communicating with a certification authority, to obtain a certificate for

the new user based on the key pair" in (Col 19 line 35 to Col 20 line 5); and "storing the certificate and the key pair for the new user in a location that is accessible by the signature server to enable the signature server to sign items on behalf of the new user" in (Col 20 lines 40-45).

12. As per claims 9, 20, and 31:

Dickinson discloses "The method of claims 1, 12, and 23, wherein the method further comprises configuring the signature server to delete an old user by: receiving a request from an authorized entity to delete the old user; notifying a certification authority to revoke a certificate .for the old user; and removing the private key for the old user from the signature server, so that the signature server can no longer sign items on behalf of the old user" in (Col 19 lines 1-9).

13. As per claims 10, 21, and 32:

Dickinson discloses "The method of claims 1, 12, and 23, wherein the method further comprises archiving the message and the signed item at the signature server" in (Col 26 lines 39-53).

14. As per claims 11, 22, and 33:

Dickinson discloses "The method of claims 1, 12, and 23, wherein the method further comprises forwarding the signed item to an archive server in order to be archived" in (Col 30 lines 35-49).

Response to Arguments

1. Applicant's arguments filed 06/26/06 have been fully considered but they are not persuasive.

2. As per remark on pages 9-10, Applicant argues that Dickinson does not disclose receiving a user identifier and an application identifier at a signature server, and looking up a private key for the user based on the user identifier and the application identifier, wherein looking up a private key for the user based on the user identifier and application identifier prevents a user who is allowed to access a second application, but who is not allowed to access the application being used, from gaining access to the application being used. Examiner disagrees with the Applicant. Dickinson does disclose the implementation of user identifier or user identification (Col 7 lines 7-30) and an application identifier, which identifies what type of algorithm to be used to sign the message (See Col 21 lines 25-40). Both the user identification (Col 7 lines 7-30) and the application identification (certificate type in (Col 21 lines 25-40)) get authenticated to retrieve the private key corresponding the certificate owned by the user (Col 21 lines 43-60). Each certificate corresponds to a private key and each certificate correspond to a cryptographic application or communication protocol, or protocol. Thus, one private key corresponds to a first certificate cannot be used for a second certificate. Therefore, Dickinson discloses the instant claimed invention clearly. See rejection above.

Conclusion

3. Applicant's amendment necessitated the new ground(s) of rejection presented in this Office action. Accordingly, **THIS ACTION IS MADE FINAL**. See MPEP § 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the date of this final action.

15. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Linh LD Son whose telephone number is 571-272-3856. The examiner can normally be reached on 9-6 (M-F).

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Kim Vu can be reached on 571-272-3859. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Linh LD Son
Examiner
Art Unit 2135

KIM VU
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100